

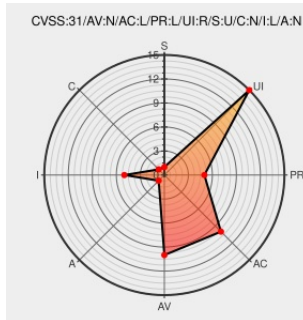


CVE-2022-4523

Published on: Not Yet Published

Last Modified on: 12/21/2022 01:15:00 PM UTC

CVE-2022-4523

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Virtual Exim 2](#) from [Virtual Exim Project](#) contain the following vulnerability:

A vulnerability, which was classified as problematic, has been found in vexim2. This issue affects some unknown processing. The manipulation leads to cross site scripting. The attack may be initiated remotely. The name of the patch is 21c0a60d12e9d587f905cd084b2c70f9b1592065. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-215903.

CVE-2022-4523 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
CVE-2022-4523 vexim2 cross site scripting (ID 274)	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?id.215903
Merge pull request #274 from rimas-kudelis/xss-prevention · vexim/vexim2@21c0a60 · GitHub	github.com text/html	MISC github.com/vexim/vexim2/commit/21c0a60d12e9d587f905cd084b2c70f9b1592065
Use `htmlspecialchars()` to escape user-provided vars before output by rimas-kudelis · Pull	github.com text/html	MISC github.com/vexim/vexim2/pull/274

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Virtual Exim Project	Virtual Exim 2	-	All	All	All
cpe:2.3:a:virtual_exim_project:virtual_exim_2:-:*:*:*:*:*::						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2022-4523	2022-12-15 22:43:48

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)